Missouri Department of Health and Senior Services

HIV/AIDS SURVEILLANCE PROGRAM CONFIDENTIALITY AND SECURITY MANUAL

REVISED OCTOBER 29, 2003

PREFACE

Within the state of Missouri, three HIV/AIDS surveillance units located in Jefferson City, Kansas City, and St. Louis City are responsible for implementing and operating comprehensive HIV/AIDS surveillance programs to reduce the spread of HIV infection and its impact on at-risk populations. Jefferson City is the administrative headquarters for all state surveillance activities and conducts surveillance in the Outstate area (108 counties). Kansas City conducts surveillance in a nine county region that includes four counties in Kansas. St. Louis City conducts surveillance in St. Louis City and St. Louis County, Missouri. Surveillance program activities guide prevention policy decisions, target prevention resources, and assist in evaluating prevention and treatment activities. All three surveillance units collaborated to develop this document that is intended to provide guidelines for management of confidential patient information within the context of all state surveillance activities.

This manual serves as the official confidentiality security policy of the Missouri Department of Health and Senior Services (DHSS) that pertains to HIV/AIDS data. These policies encompass all agencies that contract with the DHSS.

I. GENERAL BACKGROUND AND ASSURANCES

A. DEFINITIONS

1. **AIDS:** Acquired Immune Deficiency Syndrome.

2. **Confidential Information/Material:** All HIV/AIDS information is inherently confidential and is considered as some of the most confidential information managed by state and local health departments. Confidential information is considered as any information that could either directly (e.g., patient identifiers) or indirectly (e.g., small cell aggregate data) lead to the identification of a person reported with HIV/AIDS, or any other person whose identity was learned through a case investigation, case report, personal interview, database, or research study.

3. **Contractor (Contractual Employees/Agreements):** Entities funded to perform HIV/AIDS case surveillance through contractual agreements with DHSS. Current relationships exist with Kansas City Health Department (KCHD) and St. Louis City Department of Health and Hospitals (SLCHD).

4. **HIV:** Human Immunodeficiency Virus.

5. **HARS (HIV/AIDS Reporting System):** National, statewide, and local database for conducting HIV/AIDS case surveillance.

6. **Immediately:** With respect to reporting all breaches or suspected breaches of confidentiality (whether local health department to state health department or state health department to CDC), immediately is defined as within the same working day. If an event occurs late in a working day, the statewide and/or local ORPs are to be notified after normal working hours as soon as possible after the event occurs.

7. **Office of Surveillance (OoS):** This organization performs statewide surveillance for communicable, zoonotic, and environmental health conditions and is located organizationally within the Division of Environmental Health and Communicable Disease Prevention (EHCDP), Missouri Department of Health and Senior Services (DHSS) central office. OoS is responsible for conducting all statewide HIV/AIDS surveillance activities.

8. **Overall Responsible Parties (ORPs):** Designated individuals at DHSS and local contractual sites who are ultimately responsible for the security and confidentiality of HIV/AIDS surveillance information.

9. **Security (Secured):** All measures implemented to prevent access to confidential material by unauthorized individuals as described in this document. Examples of security include physically secured facilities, restricted access areas, password-protected databases, and HIV/AIDS surveillance staff training.

10. **Unauthorized Release/Disclosure of HIV/AIDS Surveillance Information:** All release/disclosure of HIV/AIDS surveillance information not authorized by the ORP as defined in section IV, A and C of this manual.

B. LEGAL BACKGROUND FOR SECURITY/CONFIDENTIALITY OF HIV/AIDS SURVEILLANCE INFORMATION

1. **Federal Regulations.** At the national level, HARS is protected by a Federal Assurance of Confidentiality of Public Health Service Act, 42 U.S.C. 242k and 242m(d), that prohibits disclosure that could be used to directly and indirectly identify patients.

2. **State Reporting Regulations.** At the state level, multiple regulations dictate HIV/AIDS reporting, security/confidentiality, and are described below:

   a. Physician Reporting-19 CSR 20-26.040. Physicians or their designates are required to report all conditions listed in 19 CSR 20-20.020 including HIV infection as indicated by HIV antibody testing (reactive screening test followed by a positive confirmatory test),

HIV antigen testing (reactive screening test followed by a positive confirmatory test), detection of HIV nucleic acid (RNA or DNA), HIV viral culture, or other testing which indicates HIV infection; newborn infants whose mothers are infected with HIV; HIV test results (including both positive and negative results) from children less than two years of age whose mothers are infected with HIV; AIDS; CD4 lymphocyte counts; and HIV viral load measurements. Providers are protected from any civil liability for reporting under RSMo. 191.656, Subsection 7.

b. Laboratory Reporting-19 CSR 20-20.080. Laboratories are required to report any positive test or any test indicative of conditions listed in 19 CSR 20-20.020 including the above tests for HIV infection, AIDS, CD4 lymphocyte counts, and viral load measurements.

c. Exemptions to Reporting-19 CSR 20-26.040. Exemptions from HIV/AIDS case reporting include: (1) all research institutions obtaining Institutional Board Approval (IRB) for a specific study with notification of the board's approval submitted to the department in writing prior to commencement of study; or (2) where prohibited by federal law or regulation.

d. State Statutes which Address Authorized Release of Surveillance Information. Specific entities to which HIV/AIDS surveillance data can be released are described in section IV, A and C.

1). RSMo.191.656. HIV/AIDS patient information can only be released to public employees with a need-to-know in order to perform their duties or private employees entrusted with patient care. Additional exceptions are outlined Subsection 2. (1) of RSMo.191.656 (Attachment 1).

2). RSMo.191.677. State statute RSMo.191.677 (Attachment 2) allows release of information by court order to allow for the prosecution of individuals who knowingly transmit HIV infection.

3). RSMo.191.658. This statute (Attachment 2a) may allow release of HIV information (if on file) to a health care practitioner providing treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or body fluids.

e. Penalties for Unauthorized Release of Surveillance Information.

1). Penalties for unauthorized release of HIV/AIDS patient information are classified as (1) negligent violation and (2) willful, intentional, and reckless violation. Negligent violation can result in a fine of $1,000, including all associated court costs and reasonable attorney fees. This is in addition to other relief the court may

judge appropriate. Willful violation can incur a fine of $5,000, including exemplary damages, court costs and reasonable attorney fees, in addition to other relief the court may deem appropriate.

2). Breach of security and confidentiality pertaining to HIV/AIDS surveillance information may result in suspension, demotion, or termination based on the severity of the offense. Severity of offense and disciplinary action for all DHSS staff with access to HIV/AIDS surveillance information is determined by the statewide ORP. Local health department administrators may elect to consult with DHSS administrators to determine the severity of offense and disciplinary action for employees of local contractual sites. The basis for disciplinary actions for DHSS staff is found in the DHSS administrative manual, Chapter 10, Section 10.4 (Attachment 3).

3). Penalties for contractual programs that breach confidentiality of HIV/AIDS surveillance information may include a reduction or loss of federal and/or state funding.

C. CONFIDENTIALITY ASSURANCES

Figure 1. Confidentiality Assurances

- **Confidentiality Oaths**
- **Overall Responsible Parties (ORPs) and Responsibilities**
- **Surveillance Staff Responsibilities**
- **Employee Identification Badges**
- **Performance Appraisals**
- **Contractual Staff**
- **Penalties for Unauthorized Disclosures**
- **Training**

1. Signing of Confidentiality Oath. All statewide surveillance staff and non-surveillance staff authorized to access HIV/AIDS surveillance information sign a health department confidentiality statement upon hire. In addition, all surveillance staff and other staff who have access to confidential data (e.g., STD Disease Intervention Specialists, Tuberculosis Control staff, designated information systems specialists in DHSS and in contractual sites) annually sign a confidentiality oath pertaining to HIV/AIDS surveillance information (Attachments 4, 5, 6, 7, and 8) and receive a confidentiality packet as described in this section, number 8. The signed (original) confidentiality statement is retained in the employee's personnel file and a copy is given to the employee.

2. Designation of Overall Responsible Parties (ORPs) and Responsibilities. DHSS has identified statewide (Figure 2) and contractual (Figure 3) Overall Responsible Parties (ORPs) who are ultimately responsible for the confidentiality and security of HIV/AIDS surveillance information.

Figure 2. Statewide ORPs

Statewide:
(Primary):
Bryant McNally, JD, MPH, Director
Division Environmental Health and Communicable Disease Prevention

(Secondary):
Garland Land, MPH, Director
Center for Health Information Management and Epidemiology

Statewide ORPs: Specific responsibilities of the statewide ORPs include:

a. Exercising the authority to make decisions about the overall HIV/AIDS surveillance operation that affect how surveillance information is collected, stored, analyzed, released, and disposed. Decisions also include which programs outside of HIV/AIDS surveillance are authorized to access surveillance data for public health purposes. This includes both DHSS central office and contractual sites.

b. Collaborating closely with the Program Manager (Yelena Friedberg) and Chief, Office of Surveillance (Lyn Konstant) to annually certify that all CDC program requirements are met. Annually completing CDC's certification form (Attachment 9).

c. Collaborating closely with Y. Friedberg and L Konstant to immediately report all breaches of confidentiality to the Chief of the Reporting and Analysis Section (Dr. Lisa Lee), HIV Incidence and Surveillance Branch, CDC.

d. Collaborating with Y. Friedberg and L. Konstant to take appropriate disciplinary action toward central office surveillance staff and surveillance contractual entities that breach the confidentiality of HIV/AIDS surveillance information. The statewide ORP will also collaborate with managers of other DHSS programs whose employees breach confidentiality of HIV/AIDS surveillance information to establish appropriate disciplinary action.

State and local health department administrators will consult with their Department's General Counsel to determine whether a breach warrants reporting to local and state law enforcement agencies.

Local ORPs:

Based on the fact that SLCHD and KCHD are contractual, remote HARS sites, DHSS is requesting that these health departments designate an individual to serve as the ORP for their respective surveillance jurisdictions (Figure 3). Local ORP responsibilities include:

Figure 3. Local ORPs

SLCHD:
Akan Ukoennin, Chief
Communicable Disease Program

KCHD:
Ron Griffin, MPH, Chief
Division of Communicable Disease and Prevention

a. Certifying annually that all CDC program requirements are met for their surveillance jurisdiction. Annually completing DHSS's certification form (Attachment 10).

b. Assuring ongoing jurisdiction adherence to all policies/procedures in Missouri's *HIV/AIDS Confidentiality and Security Manual*.

c. Collaborating closely with L. Konstant and Y. Friedberg to immediately report and resolve all breaches of confidentiality pertaining to HIV/AIDS surveillance data within their surveillance jurisdiction.

d. Ensuring that all staff managing HIV/AIDS surveillance information are appropriately trained in all aspects of security and confidentiality.

3. **Delineation of Surveillance Staff Responsibilities.** Surveillance staff has the following general responsibilities pertaining to the security and confidentiality of HIV/AIDS surveillance information:

a. Challenging unauthorized users of HIV/AIDS surveillance data. Authorized users and authorized use of HIV/AIDS surveillance information are defined in section IV of this manual, A and C.

b. Immediately reporting all suspected breaches of confidentiality to the statewide ORP or designate. DHSS central office surveillance staff should report all breaches or suspected breaches of confidentiality to L. Konstant or Y. Friedberg. Staff in local contractual sites should report all breaches or suspected breaches of confidentiality to their designated local ORP who will then immediately notify the statewide ORP or designate.

c. Exercising good judgment in the daily management of HIV/AIDS surveillance information. From time to time, confidentiality and security issues related to HIV/AIDS surveillance data may arise that are not specifically addressed in this manual. When these issues arise, surveillance staff is responsible for notifying the statewide ORP (or local ORP for contractual sites) whom can provide the necessary guidance related to these issues.

d. Ensuring confidentiality of individual surveillance workstations.

Specific surveillance staff responsibilities pertaining to security/confidentiality of surveillance data are listed in the "Workplace HIV/AIDS Security Checklist" (Attachment 11).

4 **Displaying of Employee Identification Badges.** HIV/AIDS surveillance staff statewide is required to display identification badges specific to their health department(s). These badges are required to be worn at all times when surveillance staff are working within the surveillance unit and also when conducting official activities away from the surveillance unit.

5. Administration of Performance Appraisals. Confidentiality is listed as a job component on all OoS and contractual staff performance appraisals.

6. Evaluation of Confidentiality/Security at HIV/AIDS Contractual Sites. Assurance of confidentiality is listed in annual HIV/AIDS surveillance contracts with the SLCHD and KCHD. OoS conducts biannual site visits with contractors to evaluate delivery of service, one area being confidentiality and security of HIV/AIDS surveillance information.

7. Description of Penalties for Unauthorized Disclosure of HIV/AIDS Surveillance Information. Penalties for unauthorized disclosure of HIV/AIDS patient information are outlined in I.,B.,2.,d.

8. Training for HIV/AIDS Confidentiality/Security

a. New Employee Orientation. All new surveillance staff and non-surveillance staff authorized to access HIV/AIDS surveillance information are given a confidentiality orientation and are provided the following items:

- *HIV/AIDS Security and Confidentiality Manual*
- DHSS Rules Pertaining to HIV/AIDS (including penalties for unauthorized disclosure)
- "Workplace HIV/AIDS Security Checklist"
- HIV/AIDS Surveillance Program Confidentiality Statements

During the orientation, all new surveillance staff is thoroughly trained on the methodology of HIV/AIDS surveillance including protocols for HIV/AIDS security/confidentiality. All training occurs before administrative access is granted to confidential information. Dates of security orientation are documented in each employee's personnel file.

b. Annual Updates/Trainings. Confidentiality updates/reviews are held annually during one of the statewide HIV/AIDS surveillance meetings. Updates allow for sharing of

information regarding confidentiality/security including discussion of new policy, review of existing policy, review of CDC program requirements, discussion of areas of perceived weakness within the statewide program, and discussion of contractual and individual penalties for unauthorized disclosure of confidential information. All non-surveillance staff authorized to access surveillance information is also provided confidentiality and security training on a periodic, established basis.

c. **Other Trainings.** Surveillance staff statewide attend all CDC recommended or required confidentiality trainings.

II. PHYSICAL SECURITY

A. BUILDING/RESTRICTED ACCESS AREA SECURITY

Access to all restricted areas is limited to surveillance staff or other authorized individuals (e.g., program administrators, data managers) who have a need for access. Keys and/or electronic access cards are issued to surveillance staff upon hire and are surrendered to designated administrative staff upon either resignation or termination.

1. **Office of Surveillance (OoS)**. OoS is located in one of three buildings operated by DHSS. Access to each building during normal business hours (defined as 6:30 am to 5:30 pm Monday through Friday) is through one entrance. All visitors are required to register at the front information desk and to display a visitor identification badge. OoS (and thus the HIV/AIDS surveillance unit) is located within the EHCDP work area. This work area requires electronic access through two additional doors. OoS staff must accompany visitors in order to enter the unit. Outside windows are secure. There is no dedicated area for performing HIV/AIDS surveillance activities; however, HARS and other confidential databases are housed on a confidential LAN server located within the DHSS Office of Information Systems (OIS) area, not on individual workstations. OIS is located in a separate building from the EHCDP work area and the fileserver is located within an electronically secured room with limited numbers of information systems administrators granted security clearance to this room. All DHSS entrances in addition to the EHCDP work area also require electronic access after hours and on weekends of which only a limited number of individuals have access (including cleaning crews). In the event that an access card is lost or stolen, it is immediately reported to the EHCDP Assistant Director (S. Jenkins) who is responsible for reporting the lost/stolen card to the security company.

2. **St. Louis City Department of Health and Hospitals (SLCHD).** The HIV/AIDS surveillance unit is located within the Metropolitan St. Louis AIDS Program on the fourth floor of the SLCHD. Therefore, the unit is not accessible by window. The surveillance unit is a restricted access area with double-locked doors. Both the building and the unit are locked after normal working hours (defined as 8:00 am to 5:00 pm, Monday through Friday). A security guard is posted in the building twenty-four (24) hours a day and all authorized health department staff is required to sign-in for access after normal working hours. The surveillance unit is locked if no one is present within the unit. Cleaning crews do not access the surveillance unit after normal working hours. The LAN fileserver for HIV/AIDS surveillance information is located in a double-locked service room on the seventh floor of the health department, of which several data administrators (information specialists) have access. The office is locked when vacant.

3. **Kansas City Health Department (KCHD).** The HIV/AIDS surveillance unit is located in the Communicable Disease Prevention Unit on the second floor of the KCHD. All outside windows are secure. All health department visitors are required to register at the information desk and to display a visitor's identification badge. Security guards are posted in the health department twenty-four hours daily and security cameras monitor physical grounds at all times. The Communicable Disease Prevention unit is a restricted access area and is locked during normal working hours (defined as 8:00 am to 5:00 pm., Monday through Friday); however, there is no dedicated area for performing HIV/AIDS surveillance activities. The two terminals for conducting surveillance activities are located in a cubicle-sectioned corner of the Communicable Disease Prevention Unit**.** The LAN fileserver is located within a locked room on the fourth floor and maintained by the data administrator who is the only person who has access (in addition to cleaning crews). HARS and other confidential databases are not maintained on individual workstations. All entrances to the KCHD require electronic access after hours and on weekends of which only four (4) individuals from the Communicable Disease Prevention Unit have access. In addition, a key is required to gain access to the unit itself.

B. OFFICE/SURVEILLANCE UNIT SECURITY

1. Retention of Hard Copy Files

a. All surveillance units retain hard copy files of HIV/AIDS surveillance information. All hard copy information is stored in locked filing cabinets and is accessible only by HIV/AIDS surveillance staff. All original hard copy files are housed in locked filing cabinets at the DHSS central office in Jefferson City.

a. Hard copy documents are concealed or locked up when employees are absent from individual workstations for even brief periods of time.

2. **Keys to Hard Copy Storage.** Designated staff in each surveillance unit retains the keys to hard copy storage. However, all surveillance staff is responsible for insuring security of their individual workstations, including appropriate storage of hard copy files.

III. COMPUTER SECURITY

A. DATABASE SECURITY

1. HARS is the primary database for HIV/AIDS surveillance tracking. Other supplemental databases (e.g., death certificate, pending case, d-base 5.0) are internally designed and used for epidemiological tracking. Access to all databases is restricted to HIV/AIDS surveillance personnel via password protection.

2. All surveillance units have information system specialists (data administrators) responsible for maintaining all network and database security and integrity. In the DHSS central office, these individuals are organizationally located within and outside of the HIV/AIDS surveillance unit. In St. Louis and Kansas City, these individuals are organizationally located outside of the HIV/AIDS surveillance unit (e.g. health department director's office).

3. All surveillance units possess different configurations for network security and are outlined in Figure 4. In no surveillance unit is HARS maintained on individual workstations.

Figure 4. HIV/AIDS Surveillance Network Configuration by Surveillance Unit

MDHSS:	Connected to DHSS LAN (network), DHSS Office of Information Systems (OIS) administers fileserver containing HIV/AIDS surveillance information. Surveillance utilizes trustee rights to confidential volume on fileserver.
St. Louis City:	Connected to SLCHD LAN (network), the STD Control Program and the HIV/AIDS Surveillance Program share a confidential server.
Kansas City:	Connected to KCHD LAN (network), surveillance utilizes trustee rights to confidential volume on fileserver.

B. PC WORKSTATION SECURITY

1. All surveillance staff is responsible for protecting his/her workstation (terminal) containing HIV/AIDS surveillance information. This includes protecting individual passwords that would allow access to confidential information/data.

2. Terminals for all statewide HIV/AIDS surveillance staff are single password protected. Passwords in all surveillance jurisdictions are at least a minimum of five characters. On an established basis in each jurisdiction, users change passwords to insure database security.

Access to HARS and other confidential databases are restricted to HIV/AIDS surveillance personnel via group access authority and network password protection.

3. All surveillance staff log off the network at the end of each day or when leaving the office for extended periods of time (defined as 2 hours or more). In the event a user fails to log out, networks at SLCHD, KCHD and DHSS automatically log off users after a specified time.

4. OoS terminals utilize privacy screens due to workstation configurations.

5. At DHSS, retention of any confidential information (other than the information contained in HARS) is maintained on secured drives. At KCHD, confidential information in addition to HARS is stored in d-base (a major supplemental database). Also, the secured drive is used to store nightly back-ups of HARS. Secured drives are protected, and access is restricted to the user group. The data manager or designated information specialists of DHSS, SLCHD and KCHD also have access. Secured drives are not needed at SLCHD due to network configuration.

6. All disks and computer hard drives are cleaned prior to surplus with Norton's WipeInfo (Government Erase). At DHSS, DHSS Office of Information Systems (OIS) staff prior to surplus also checks all hard drives for confidential information.

7. Anti-virus software is installed on all terminals at DHSS, SLCHD, and KCHD. Surveillance staff is responsible for reporting all computer viruses or suspected computer viruses to their designated information systems staff.

8. All surveillance system hardware (fileservers) is located in areas that are adequately regulated with respect to temperature to avoid software/hardware damage.

IV. DATA CONFIDENTIALITY AND SECURITY

A. RELEASE OF DATA TO NON-HIV/AIDS SURVEILLANCE STAFF

1. All data released is in accordance with RSMo.191.656**,** 191.677 and 191.658 that provides general guidelines for the release of HIV/AIDS surveillance information. This manual approved by the statewide ORP, lists specific protocols and policies for the release of HIV/AIDS surveillance information.

2. All surveillance staff is required to exercise discretion when releasing any surveillance data. Surveillance staff should consult with the local or statewide ORP (or designate) if they have questions pertaining to release of HIV/AIDS surveillance information.

3. All surveillance information pertaining to a specific HIV/AIDS case may be released to known, authorized providers (including infection control practitioners) directly involved in the health care of a patient.

4. All surveillance information may be released to authorized out-of-state surveillance staff for the tracking of a patient within their jurisdiction.

5. Confidential information may be released to other agencies within or outside DHSS who require such information to perform their job responsibilities (Figure 5).

Figure 5. Agencies in Missouri Obtaining Confidential HIV/AIDS Information

- STD Program
- TB program
- Medicaid Waiver Program
- HIV Case Management
- State and Local Prosecuting Agencies

a. Sexually Transmitted Disease Control Program. In Missouri, HIV/AIDS surveillance data are linked with partner notification activities for sexually transmitted diseases including HIV. Designated surveillance staff provide in-state and local contractual Disease Intervention Specialists (DIS) with only the patient information (demographic, clinical, and risk) needed to perform an effective field investigation. Surveillance staff also shares information with out-of-state STD Control programs for the same reason. The efforts of DIS identify contacts to known cases and therefore can potentially identify new cases of HIV infection. When required, DIS also has an integral role in resolving NIR (no-identified risk) investigations. Exchange of information between HIV/AIDS surveillance staff and DIS staff is bilateral and occurs on both the state and local levels.

b. Tuberculosis Control Program. In the DHSS central office on a quarterly basis, names and dates of birth of all tuberculosis infection, tuberculosis disease and mycobacterium other than tuberculosis (MOTT) cases are matched electronically to names and dates of birth of cases in HARS. Designated HIV/AIDS surveillance staff conducts the match. If an individual has dual diagnoses (i.e., TB/MOTT and/or HIV/AIDS), the diagnosis and RVCT number is noted on the patient record in both the tuberculosis and HARS registries. Hardcopy HIV/AIDS case reports are not shared with the tuberculosis program staff.

The KCHD HIV/AIDS Surveillance Program obtains names, dates of birth, and diagnosis of persons with tuberculosis disease or MOTT from the local tuberculosis program. After HARS is record searched and the appropriate co-morbidity updated in HARS, the tuberculosis program is then notified of the dual diagnosis of either HIV or AIDS. The tuberculosis program uses a numerical code to indicate those persons with co-morbidity (a three digit number which is used in place of the words “HIV or AIDS”).

The SLCHD HIV/AIDS Surveillance Program does not receive any information from their local tuberculosis program. Tuberculosis disease and MOTT updates are received on hardcopy from Jefferson City. This information is shredded after local entry into HARS.

c. Missouri Medicaid Waiver Program. Upon request, designated HIV/AIDS surveillance staff confirms the HIV diagnosis of individuals receiving services under the Medicaid Waiver Program and report the status to designated Medicaid Waiver staff. Only confirmation of either HIV/AIDS diagnosis is provided to Medicaid waiver staff, no additional surveillance information. Medicaid information can also be a potential case finding/validation source for the Missouri surveillance program. Release of this information only occurs on the state level.

d. HIV Case Management Program. Upon request, HIV/AIDS surveillance staff verifies the diagnosis of individuals who apply for Missouri HIV case management services. Case management links HIV diagnosed clients to care, community resources, and information. Confirmation of HIV/AIDS diagnosis (including appropriate laboratory information, CD4 counts, viral loads, and opportunistic infections) is provided to designate case management staff. Additional surveillance information (e.g., partner notification activity) may be provided if requested to assist with comprehensive patient management. Case management is also a valuable case finding/validation source for the Missouri surveillance program. Release of this information occurs on both state and local levels.

e. State and Local Prosecuting Agencies. Upon request, HIV/AIDS surveillance information can be released to state and local prosecuting attorneys to enforce RSMo. 191.677. Release is coordinated by the Chief, OoS with DHSS General Counsel. The only information released to prosecutors is laboratory history to verify the status of the prosecuted individual. Release of information occurs only on the state level.

6. DHSS does not release HIV/AIDS surveillance information to law enforcement officials (e.g., defense attorneys, prosecuting attorneys, and detectives) not described under the scope of RSMo.191.677 without a subpoena or court order, depending on the exact nature of the request. The statewide ORP or designate collaborates closely with the DHSS Chief Counsel to respond to all named-identifier requests from law enforcement. DHSS Chief Counsel collaborates with the State's Attorney General's Office to resist all such release of HIV/AIDS surveillance information. Local contractual agencies are required to refer all requests from law enforcement to the statewide ORP or designate.

7. According to state statute, RSMo.191.658, a health care practitioner, providing medical treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or other body fluids that occurred in the course of the

worker's or officer's employment, may request from the department of health, information regarding the HIV infection status of the source individual.

A protocol has been established for operationalizing the requirements of this statute and to reduce to a minimum the number of times the state registry is used to determine the status of a source individual. Local contractual agencies and central office staff are required to refer all requests from providers to the statewide ORP or designate. These requests are then routed to one of the designated state HIV consultants (e.g., consultant community health nurse, medical epidemiologist) who will determine if a significant exposure, as defined in the law, has occurred and if HIV information on the source individual is essential in providing necessary medical treatment. The caller will be provided with appropriate treatment recommendations and other medical information (e.g., assure the exposed individual is evaluated for hepatitis B and C as well as HIV, referring to CDC recommendations for post-exposure prophylaxis).

If the information collected meets the criteria set forth in the law and it is determined that the source person's HIV status is needed in order to determine or encourage ongoing appropriate treatment for the exposed individual, information on the exposed individual will be obtained (e.g., name, date of birth, race). This information will be referred to authorized staff in OoS who have access to the HIV/AIDS database (Section C., Figure 4). Only those individuals with access to the HIV/AIDS database will know if the source patient is infected with HIV and will have the responsibility to notify the provider of the results.

8. State statute (RSMo.191.689) requires school notification of children with HIV infection, only after a school has adopted a policy consistent with recommendations of CDC on school children that test positive for HIV. In view of concerns related to patient confidentiality, the HIV/AIDS surveillance program does not operationalize the statute.

9. Named HIV data are not released to researchers unless they sign the DHSS HIV/AIDS surveillance program confidentiality statement and are conducting a DHSS Institutional Review Board (IRB) approved project.

10. De-identified HIV/AIDS surveillance data sets are provided to statewide and local epidemiologists for the analysis of HIV/AIDS surveillance data.

11. The statewide HIV/AIDS surveillance program exercises great caution in public release of numerical, small cell data that could either directly or indirectly lead to the identification with a person infected with HIV/AIDS. Several independent variables (e.g., risk factor, race, age) could lead to the direct/indirect identification of a person with HIV/AIDS and should be carefully evaluated in view of the total population of the jurisdiction under observation including racial and risk distribution/prevalence. For the central office program, no small cell data are released without consent from the Program Manager and/or the Chief of the

office. In contractual sites, no small cell data are released without the consent of the local ORP or designate.

B. TRANSFER OF HIV/AIDS SURVEILLANCE DATA

1. **Contractors.** HIV/AIDS Surveillance contractual sites monthly transfer completed HIV/AIDS case forms and other confidential information to OoS. Transfer is performed in two forms: hardcopy and electronic. Regarding hardcopy transfer, both contractual sites mail all hard copy data (i.e., completed HIV/AIDS case report forms, laboratory results) in double envelopes via certified mail. Both contractual sites (SLCHD and KCHD) electronically transmits cases via password protected E-mail. OoS mails all confidential hard copy information to contractors in double envelopes sent via certified mail.

2. **CDC.** OoS forwards all new and updated entries on HARS records to CDC monthly via password protected E-mail. Patient names are not forwarded to CDC.

C. AUTHORIZED STATEWIDE HIV/AIDS SURVEILLANCE STAFF WITH ACCESS TO HARS

Only authorized staff performing HIV/AIDS surveillance responsibilities has **direct** access to HARS. Authorized surveillance staff for all three units and defined functions within that unit are listed in Figure 6.

Figure 6. Statewide Personnel* with Authorized Access to HARS and Function

OoS	Statewide HIV/AIDS Research Analyst HIV/AIDS Surveillance Specialist (Outstate Core Surveillance) HIV/AIDS Database Manager (Statewide QA, Entry of Outstate Case Reports, Preparation of Statistical Reports) Two Support Staff (Laboratory Data Entry) Two Data Managers (Data Administration)
St. Louis City	HIV/AIDS Surveillance Coordinator (Preparation of Statistical Reports) HIV/AIDS Surveillance Specialist (City/County Core Surveillance) HIV/AIDS Surveillance Support (Laboratory Data Entry)
Kansas City	HIV/AIDS Surveillance Coordinator (HIV/AIDS Case Surveillance, Data Entry, Preparation of Statistical Reports)

* Systems administrators in all three areas have access to HARS for fileserver maintenance but HARS is not accessed on a routine basis.

D. BACK-UPS OF HIV/AIDS SURVEILLANCE DATA

Back-ups are performed regularly in all surveillance jurisdictions.

1. **DHSS.** At DHSS, OIS completes a full back-up of all computer volume for DHSS users once a week, with incremental back-ups daily. Data are saved on tapes that are stored in a locked room within the OIS unit. Incremental back-ups are kept for one week, full back-ups are kept for one month; the last full back-up on the last day of the month is kept indefinitely in an offsite safe which only two OIS system administrators have access.

2. **SLCHD.** At SLCHD, the surveillance support clerk backs up the HARS database on diskettes at the end of a two-week period. The same disk is used when the next back up occurs (data overwritten). The disks are stored in a filing cabinet within the locked surveillance unit.

3. **KCHD.** At KCHD, the AIDS surveillance coordinator backs up HARS nightly on a secured drive. Each nightly back-up is kept for one week and is then overwritten by the current week's data

E. DISPOSAL OF HIV/AIDS SURVEILLANCE DATA

1. All hard copy confidential information (e.g., CD4-lymphocyte, viral load reports, notes from medical record reviews) is shredded when no longer needed.

2. All disks and computer hard drives are cleaned prior to surplus with Norton's WipeInfo (Government Erase).

F. PHOTOCOPYING/PRINTING OF HIV/AIDS SURVEILLANCE DATA

Confidential information is not left unattended in common access areas and is retrieved immediately upon copying/printing.

V. RAPID COMMUNICATION

A. ELECTRONIC

1. **Facsimile.** Facsimile is used in all surveillance units to communicate confidential information. When confidential information is faxed outside the surveillance unit, all staff

assures that the recipient has a dedicated facsimile line or is contacted prior to transmission. Confidential material faxed to outside sources contains a generic health department cover sheet that contains a notice of confidentiality. Neither the cover sheet nor faxed material has any direct or indirect reference to HIV/AIDS. If incoming faxes are not received within the expected time, surveillance staff contacts the sender. The KCHD HIV/AIDS surveillance program does not have a dedicated facsimile line. However, only HIV/AIDS surveillance staff retrieves faxes containing confidential information. DHSS and the SLCHD do have dedicated facsimile lines.

2. **E-mail.** E-mail may be used to transmit named identifying information to other DHSS staff or contractors using PK-zip with password protection (data encryption method). E-mail is utilized to transmit HARS data electronically from both contractual sites to DHSS. In addition, OoS transmits new and updated entries on HARS records to CDC via E-mail.

B. MAIL

1. **Incoming-** All incoming department mail is opened in the mail opening room. Four persons work in this room. These persons are required to sign the department confidentiality statement; however, the director of the department made the decision that it wasn't necessary for these individuals to sign the HIV/AIDS confidentiality statement. The mail is then opened and date stamped by these individuals. If it's considered safe mail, it's put in a slot in the safe room. When all mail is opened, and considered safe, it is then put in a gray tub and delivered to each section or office. On delivery, a designated person (office manager) in OoS signs a form stating that the mail has been delivered. The mail is then dispersed to designate HIV/AIDS surveillance staff. Senders of confidential information are instructed to address mail to the designated surveillance unit. Physicians and other case reporters are provided return envelopes stamped "confidential" for submitting case reports. The return envelopes have no direct reference to HIV/AIDS. Appropriate administrative personnel (e.g., Program Manager at KCHD and HIV/AIDS Surveillance Coordinators at SLCHD and OoS) should be notified of all mail routed to the incorrect health department program and appropriate health department staff and/or providers notified to prevent reoccurrence.

2. **Outgoing-** All outgoing mail containing patient identifiers is marked "confidential", double enveloped, and sent via certified mail. No outgoing envelopes have any direct or indirect reference to HIV/AIDS.

C. TELEPHONE

1. **Incoming-** Generic identifiers (e.g., "Department of Health and Senior Services", "This is Joe", "Office of Surveillance"), without any direct reference to HIV/AIDS, are used when answering all incoming calls. Confidential information is shared over the phone with individuals authorized to access HIV/AIDS surveillance information as listed in section IV,

A and C. Specific techniques (e.g., call back verification) are recommended to determine authorized individuals.

2. **Outgoing-** Confidential information is requested via phone to perform routine HIV/AIDS surveillance activities. Messages with identifying patient identifiers are not left on voice mail systems unless there is prior confirmation of a secure line. Staff discusses confidential information only in secure areas, release information to only those individuals with a need-to-know (as defined in section IV, A and C), and always use utmost discretion.

VI. FIELD ACTIVITIES

A. CONFIDENTIAL MATERIALS TRANSPORTED TO THE FIELD

1. Line-listings

a. Line-listings are routinely carried into the field to perform routine HIV/AIDS surveillance activities.

b. Surveillance information on line listings is de-identified. Although line-listings typically contain the patient name, DOB, status (HIV or AIDS), and risk information, the status and risk information is coded either alphabetically or numerically (such as the coding system used in HARS) so as to neither directly nor indirectly identify the contents of the line-list.

c. Only patient information on work to be performed for that day is transported into the field.

2. **Laptops.** Laptops are not currently used in the field for HIV/AIDS surveillance activities.

B. TRANSPORTATION OF CONFIDENTIAL MATERIALS

1. All confidential materials are carried in a secured briefcase when performing field activities. Briefcases are never left unattended including in locked vehicles.

2. Confidential information should always be returned to the HIV/AIDS surveillance unit at the close of each business day. Prior approval must be obtained from the HIV/AIDS surveillance coordinator when out-of-town travel or some other reason precludes the return of confidential information to the unit.

3. When it is absolutely not possible to return confidential materials to the surveillance unit at the close of each business day (either because out-of town travel, emergency, or for some other reason), confidential information is always stored in appropriate places (e.g., locked hotel rooms, private residences).

C. ADDITIONAL FIELD SECURITY PROTOCOLS

1. Surveillance staff always presents health department identification when performing surveillance field activities.

2. All discussions pertaining to confidential information are conducted in secure, private areas. Medical record reviews are conducted as discreetly as possible.

3. Confidential information is never left in public or general access areas.

VII. PROCEDURES FOR SYSTEMATIC REVIEW OF HIV/AIDS SECURITY AND CONFIDENTIALITY PRACTICES

A. The Program Manager has prepared a spreadsheet to evaluate statewide progress toward meeting CDC program requirements. The spreadsheet lists individual program requirements and descriptions of how they are currently being met. For those that have not been met, progress toward compliance is detailed. The spreadsheet includes all DHSS, SLCHD, and KCHD activities. The spreadsheet will be reviewed on an annual basis to insure compliance with all program requirements. Based on the review of the contents of the spreadsheet, this manual will be appropriately updated.

B. When all changes to information systems technology are proposed (e.g., fileserver configuration changes, purchase of new equipment for CDC pilot projects), information system specialists in all surveillance units are responsible for collaborating with the program manager to prepare technical solutions. This collaboration will help ensure that in no way the security and confidentiality of HIV/AIDS surveillance data are electronically compromised.